



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

aw

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/221,869	12/29/98	LINEHAN	SE9-98-031(1)

STEVEN J MEYERS
IBM CORPORATION
INTELLECTUAL PROPERTY LAW BLDG 1
ROUTE 100 MP 1L1140
SOMERS NY 10589

LM02/0510

EXAMINER

HESS, R

ART UNIT PAPER NUMBER

2764

DATE MAILED: 05/10/00

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.

09/221,869

Applicant(s)

LINEHAN, MARK

Examiner

Richard W. Hess

Art Unit

2764

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

- 1) ☒ Responsive to communication(s) filed on 29 December 1998.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 December 1998 is/are objected to by the Examiner.
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).
- a) ☐ All b) ☐ Some * c) ☐ None of the CERTIFIED copies of the priority documents have been:
1. ☐ received.
 2. ☐ received in Application No. (Series Code / Serial Number) _____.
 3. ☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

- 14) ☒ Notice of References Cited (PTO-892)
- 15) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 16) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4.

- 17) ☐ Interview Summary (PTO-413) Paper No(s) _____.
- 18) ☐ Notice of Informal Patent Application (PTO-152)
- 19) ☐ Other: _____.

Art Unit: 2764

DETAILED ACTION

1. Claims 1–45 have been examined.

Drawings

2. The drawings are objected to because of the minor informalities cited on the attached form PTO 948. Correction is required.
3. Applicant is required to submit a proposed drawing correction in reply to this Office action. However, formal correction of the noted defect can be deferred until the application is allowed by the examiner.

Specification

4. The disclosure is objected to because of the following informalities:
 - The applicant initiates a second, more detailed, description of the invention on page 13, line 31 by itemizing the protocol steps and referring to Figure 2A. However the number of itemized steps described in this section of the application do not correspond to the numbered steps shown in Figure 2A. The 2nd step shown in Figure 2A is combined with step numbered 1. It is confusing and unnecessarily difficult to read and understand this section of the invention description.
 - In the description of the split shipment variation of the invention, the applicant discusses additional message interaction between the merchant and the issuer gateway and states that Figure 4 shows this additional message interaction (page 19, line 34 through page 20, line 13). The applicant goes on to state that the split shipment message interaction begins with the Merchant sending the authorization

Art Unit: 2764

token to the issuer gateway along path 402 in Figure 4. However, Figure 4 only shows the authorization token being passed from the issuer gateway to the merchant and not in the other direction as stated in the applicant's specification.

This description and the references to Figure 4 are confusing. The same issues are present in the description of the installment features of the invention (page 21, lines 4–11). A similar discrepancy is also present in the description of the payment protocol on page 22, line 1 through page 23, line 9.

- The applicant refers to "request 1" in line 5 on page 20 of the specification. There is no "request 1" in Figure 4 or other parts of the specification.
- On page 21, lines 20–23, the applicant states that the issuer could offer special payment options to the consumer at step 2 of the protocol (3rd according to Figure 2A), however, this step is a message from the consumer to the issuer. It is not clear how the issuer could offer special payment arrangements to the consumer in a message sent from the consumer to the issuer gateway.

Appropriate corrections are required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 27 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant

Art Unit: 2764

regards as the invention. The applicant states that "Japanese Payment Options" are provided offering "special payment arrangements" to the consumer. When the examiner looks to the specification for a better definition of what is meant by the terms "Japanese Payment Options" or "special payment arrangements", the only specific definition that is available is the "offering of installment and other payment arrangements" (page 21, lines 13–28). This explanation does not particularly point out or define the metes and bounds of what the applicant means by "Japanese Payment Options", so the claim is indefinite.

For the benefit of the following art rejections, the examiner will assume that payment protocols that include periodic payments cover the scope of this claim.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1–14 and 16–45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al, US Patent 5,715,314, Elgamal, US Patent 5,671,279, Gifford, WO 95/16971, Anderson et al., "Description of Financial Agent Secured Transactions (FAST) Authentication," Financial Technology Consortium, Fourth Draft,

Art Unit: 2764

December 2, 1998 and O'Mahony et al, Electronic Payment Systems, Artech House, Inc., Norwood, MA, 1997.

As per Claim 1, Payne et al teaches an electronic network commerce system comprising the steps of:

- Sending from a merchant's computer over an Internet network (column 4, lines 43–45) to a consumer's computer, a merchant message (column 5, lines 50–53). This merchant message includes a payment amount, an order description, a merchant digital signature (column 5, lines 29–46) and a timestamp (column 5, lines 39–40). Payne et al does not explicitly state that the merchant message contains a digital certificate from an acquiring bank as claimed by the applicant. Elgamal, however, expressly teaches that the message from the merchant to the customer in his electronic commerce system contains a digital certificate from the acquirer (column 9, lines 55–59). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by including the certificate from the acquiring bank as taught by Elgamal to get the invention as claimed by the applicant. The advantage would be to provide an important form of authentication in network commerce systems (Elgamal, column 4, lines 37–42)
- Payne et al also does not explicitly teach that the merchant message is a wallet initiation message and that this message starts a consumer's wallet program in the consumer's computer in response to the wallet initiation message. However,

Art Unit: 2764

O'Mahony et al explicitly teaches that the merchant response from a consumer pay message initiates a wallet program in the consumer's computer (page 79, Section 4.6.3, paragraph 1, lines 1-5). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the wallet initiation message taught by O'Mahony et al for the advantage of making the purchasing steps as transparent as possible to the consumer by hiding the details of the payment steps and messages during a purchase (O'Mahony et al, page 78, Section 4.6.1, lines 1-4).

- Payne et al explicitly teaches sending from the consumer's computer, a message containing the consumer's identity and authentication information to a payment computer (including an issuer gateway for an issuing bank) (column 6, lines 30-43).
- Payne et al expressly teaches the issuer gateway verifies the merchant's signature to prove that the consumer is dealing with the actual merchant and validating, at the issuer gateway, the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement (column 5, lines 34-36, column 7, lines 24-27 and column 8, lines 3-5).
- Payne et al explicitly teaches that the issuer gateway verifies the consumer's account (column 6, lines 43-56) and ensures that funds and/or credit are available to support the payment amount (column 7, lines 14-15).

Art Unit: 2764

- Payne et al teaches that the payment computer (or issuer gateway) authorizes payment by sending over the Internet network an authorization token, an issuer's digital certificate, and a wallet initiation message (covered above). He also teaches that the authorization token includes the payment amount, order description, timestamp, a merchant identifier and a reference to the consumer's credit or debit card number (column 7, lines 14–30).
- Payne et al, however, does not explicitly state that the payment authorization message (token) contains a random nonce, but Gifford explicitly teaches issuing a payment order that includes a random nonce as claimed by the applicant (page 4, lines 21–28). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by including a nonce in the payment authorization as taught by Gifford for the advantage of preventing a replay attack on the payment system (see page 48, Section 3.11 of O'Mahony et al).
- Payne et al explicitly teaches that once the merchant's computer receives the authorization token, the order description is fulfilled (column 7, line 49).

As per Claim 2, Payne et al expressly states that a start message is sent from consumer's computer over the internet network to the merchant's computer, to initiate the merchant's message (Figure 2A, number 32).

As per Claim 3, Payne et al teaches that the message received from the merchant in response to a buy message contains digital signature from the merchant

Art Unit: 2764

(column 5, lines 42–43). Payne et al does not explicitly teach that the digital signature contains a nonce as claimed by the applicant. Elgamal, however, explicitly teaches that message sent from the merchant to the consumer is also signed by the merchant (column 9, lines 56–60) and the signature contains a nonce (column 8, line 16). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the inclusion of the nonce in the message sent from the merchant to the consumer as taught by Elgamal for the advantage of preventing a replay attack. The limitation that this message is a wallet initiation message was already covered in the rejection of Claim 1 above.

As per Claim 4, Payne et al explicitly teaches that the merchant's computer further performs the steps of receiving the authorization token (Figure 2H, number 92); verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token (Figure 2H, number 94); verifying the freshness of the authorization token via the timestamp in the token (Figure 2H, number 98); and fulfilling said order description (Figure 2I, number 102). Payne et al does not explicitly state that a nonce in the authorization token is used to recognize duplicate tokens as claimed by the applicant. O'Mahony et al teaches that a nonce is used to recognize duplicate tokens (page 48, Section 3.11 of O'Mahony et al). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by using a nonce as taught by O'Mahony et al for the advantage of preventing a replay attack on the payment system.

Art Unit: 2764

As per Claim 5, Payne et al explicitly teaches the use of a userid and a password to identify the consumer (column 6, lines 43–44)

As per Claim 6, Payne et al teaches that the consumer interacts with a payment computer in his network sales system, but does not explicitly state that the payment computer is an ATM or a bank. Anderson et al teaches that FAST establishes a connection between the customer and the customer's bank by using a login and password (page 3, section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the payment computer being the consumer's bank as taught by Anderson et al for the advantage of using an existing financial institution that is familiar to the consumer. Official Notice is also taken that both the concept and advantages of a bank using an ATM account debit card and password are well known and expected in the banking arts. It would have been obvious to use an ATM debit card number and PIN to identify a consumer because ATM accounts and PIN are a very common way for bank customers to interact with their bank and would avoid the confusion of creating multiple access accounts for the bank and the bank's customers.

Claims 7–13 describe a plurality of cryptographic ways to authenticate the consumer's identity in the claimed payment protocol. Official Notice is taken that both the concept and advantages of the various ways to authenticate customers in a payment system as itemized in Claims 7–13 are well known and expected in the payment and cryptography arts. It would have been obvious to have provided these

Art Unit: 2764

authentication methods because establishing the identity of a party in a payment system is an essential element in any payment system (see O'Mahony et al, pages 19 and 31).

As per Claim 14, Payne et al explicitly teaches that the issuer gateway sends the authorization token to the consumer and the consumer forwards the authorization token to the merchant (column 7, lines 31–33).

As per Claim 16, Payne et al explicitly teaches the use of an alias card number that is mapped at the issuing bank to a real card number thereby preventing use of the consumer's credit card number without the authorization token (Figure 7 and column 6, lines 15–29).

As per Claim 17, Payne et al does not expressly state the use of an authorization number in the message sent back to the merchant. Gifford teaches the use of an authorization number allocated uniquely by the issuer gateway for each authorization (page 6, lines 20–23). Gifford also teaches that the issuing bank (payment computer) maintains a database mapping of authorization numbers to card numbers, so that when the issuing bank receives the capture message, it uses the database mapping to determine the consumer's card number (page 15, lines 16–27 and Figure 13). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the authorization number system taught by Gifford for the advantage of providing added security for users who are reluctant to use their actual credit card numbers over the payment network.

Art Unit: 2764

As per Claim 18, Payne et al does not expressly state the use of an authorization token containing a dummy number for use in routing payment to an appropriate one of a plurality of issuing banks, such that the dummy card number is shared among all card holders of a particular issuing bank. Official Notice is taken that both the concept and advantages of using a dummy number (such as a bank identification number (BIN)) are well known and expected in the credit card and banking arts. It would have been obvious to use such a number because it would increase the efficiency of transmitting the electronic payment instructions through existing clearing house systems.

As per Claims 19–23, Official Notice is taken that both the concept and advantages of using various authorization certificate hierarchies are well known and expected in the electronic commerce arts. It would have been obvious to include the various certificate arrangements cited in Claims 19–23 in order to make sure that all parties in the payment protocol are trusted and are who the claim to be in any transaction.

As per Claim 24, Payne et al does not explicitly teach the payment protocol for the case of a split shipment as claimed by the applicant. Elgamal specifically covers the payment protocol for split shipments as claimed by the applicant (column 13, line 64 through column 14, line 7). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the split shipment payment protocol taught by Elgamal for the advantage of handling partial shipments.

Art Unit: 2764

As per Claim 25, Payne et al teaches that his sales system can buy a plurality of products and add these products to a shopping cart (column 7, line 55 through column 8, line 2), but he does not explicitly disclose including "Japanese Payment Options" (installment payments) as claimed by the applicant. Elgamal explicitly teaches that his payment protocol covers periodic payments (column 13, lines 53–63). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the periodic payment capability taught by Elgamal for the advantage of making car payment or other periodic payments.

Claims 26, 27 and 28 are apparatus and program code claims that contain the same limitations already covered in the rejection of Claim 1, so the same rejections apply to these Claims.

Claims 29, 30 and 31 contain the same limitations already covered in the rejections of Claims 2, 3 and 4 respectively, so the same rejections apply to the rejections of Claims 29–31.

As per Claim 32, Payne et al teaches using an account number associated with the payment computer, but does not explicitly teach using the consumer's credit or debit card number as claimed by the applicant. Elgamal, however, explicitly teaches including the consumer's credit or debit card account number in the payment instruction message (column 10, lines 1–33). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by referring to the actual consumer's credit or debit account number as taught by Elgamal

Art Unit: 2764

for the advantage of being able to directly access the consumer's account without having to go through a intermediary account translation file.

Claim 33 contains the same method steps already covered in the rejection of Claim 1, so the same rejections apply to the rejection of this Claim. The applicant, however, includes one additional limitation concerning the use of a URL to identify the network location of the acquiring bank contacted via an Internet network as part of the payment protocol. Official Notice is taken that both the concept and advantages of using a URL to locate a particular location on the Internet are well known and expected in the Internet and network communication arts, because the URL address structure has been used on the Internet since its inception.

Claim 34 contains the same limitations already covered in the rejections of Claims 1, 7-10, 18 and 23-26, so the same rejections apply to the rejection of this Claim.

Claim 35 contains the same limitation already covered in the rejections of Claims 1 and 19, so the same rejections apply to the rejection of this Claim.

Claim 36, contains the same limitation already covered in the rejections of Claims 1 and 19-23, so the same rejections apply to the rejection of this Claim.

Claims 37-39 contain the same limitations already covered in the rejections of Claims 32, 3 and 4 so the same rejections apply to the rejections of Claims 37-39.

As per Claims 40-42, Payne et al teaches the sales process but does not cover the steps necessary for a capture process in a payment protocol. Elgamal, however,

Art Unit: 2764

covers the capture process steps as claimed by the applicant in Claims 40–42 (column 11, line 43 through column 12, line 63). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the capture process taught by Elgamal for the advantage of actually settling the account between buyers and merchants as is common practice in almost any payment protocol.

As per Claim 43, Payne et al explicitly teaches hashing the order information before it is sent to the merchant and also teaches that the hashing function is known by the payment computer and the merchant (column 7, line 65 through column 8, line 2). Official Notice is taken that both the concept and advantages of the merchant validating that the authorization token refers to the same order description by comparing the hash of the order description in the authorization token against a locally-computed hash of the same order description are well known and expected in the cryptographic arts. The very nature of hashing is to assure that the hashed data has not been altered by comparing the sent hash value to the hash value obtained by the recipient of the data.

Claim 44 contains the same limitations already covered in the rejection of Claim 32, so the same rejection applies to the rejection of this Claim.

As per Claim 45, Official Notice is taken that both the concept and advantages of using higher-level security protocols such as SSL are well known and expected in the encryption arts. It would have been obvious to use higher-level security protocols such as SSL because it would allow the payment protocols to be used open public networks

Art Unit: 2764

such as the Internet. In fact SSL was developed for secure communication on the Internet (O'Mahony et al, page 72, second paragraph).

9. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al, Elgamal, Gifford, Anderson et al and O'Mahony et al, as applied to Claim 1 above, and further in view of Ogram, US Patent No. 5,822,737.

As per Claim 15, Payne et al teaches that the payment computer sends a redirect message to the buyer computer and this message is forwarded to the merchant computer (column 7, lines 31–33). Payne et al goes on to teach that a portion of the information contained in the message forwarded to the merchant is encrypted so that only the payment computer and the merchant can view the contents of the message (column 7, line 24–30). Since the encrypted portion of the message is only viewable by the payment computer and the merchant, this portion of the message would inherently be sent directly to the merchant as claimed by the applicant. Payne et al, however, does not explicitly show a direct connection from the payment computer to the merchant as claimed by the applicant. Ogram explicitly shows the direct connection between the payment computer and the merchant (Figure 2D). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the with the direct connection taught by Ogram for the advantage of making sure the message went through when the customer's computer was disconnected and the payment computer was ready to send information intended specifically for the merchant.

Art Unit: 2764

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Nelson, US Patent No. 6,058,381, teaches the use of a grantor to pre-authorize payment and communication directly from grantor to merchant. Also features extensive use of URL's and the Internet.
- Gifford, US Patent No. 6,049,785, teaches a pre-authorized payment system for purchasing goods and services over a public computer network system like the Internet.
- Kravitz, US Patent No. 6,029,150, customer communicates with an agent to authorize payment. Authorized payment information is transmitted to the vendor via the customer.
- Checchio, US Patent No. 6,023,682, teaches the use of a purchase token the contains an encrypted customer credit card number.
- Williams et al, US Patent No. 6,016,484, teaches use of wallet or purse in purchase transactions.
- Watson, US Patent No. 5,991,750, teaches the use of pre-authorization parameters in purchase and payment transactions.
- Barber, US Patent No. 5,930,777, discloses system for a consumer to purchase access to network information by the use of tokens minted by a banker.
- Gifford, US Patent No. 5,724,424, is the US version of the WO patent cited in case.

Art Unit: 2764

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Richard W. Hess whose telephone number is (703) 308-6287. The examiner can normally be reached on M-F (7:00-4:30) First Friday Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P. Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-5357 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.


James P. Trammell
Supervisory Patent Examiner
Technology Center 2700



Richard W. Hess
May 8, 2000